UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/269,830	04/01/1999	ALFRED SCHEERHORN	2345/62	1687

26646 7590 10/06/2004

KENYON & KENYON
ONE BROADWAY
NEW YORK, NY 10004

EXAMINER	
CALLAHAN, PAUL E	

ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 10/06/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)
	09/269,830	SCHEERHORN ET AL.
	Examiner	Art Unit
	Paul Callahan	2137

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *22 June 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *11-30* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *11-30* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 6-23-2004 has been entered.

2. Claims 11-30 are pending in this application and have been examined.

Response to Arguments

3. Applicant's arguments filed 6-23-204 have been fully considered but they are not persuasive.

The Applicant argues in traverse of the rejection of claim 11 under 35 USC 102(b) as being anticipated by Atalla '710 by asserting that Atalla does not teach the feature of calculating an authentication token as a function of the data *"in a communications phase"* to authenticate both the signals and a transmission sequence of the signals. The Examiner counters by noting that such is taught by Atalla in the abstract where Atalla teaches calculation of an authentication token where he states: *" The method and means...operates on the message, and a sequence number that is*

unique to the transaction message to form a message authentication code in combination with the user's personal identification number..." The transaction message taught by Atalla does fall within a reasonably broad interpretation of *"data in a communications phase"* as this terminology would be understood be a person of ordinary skill in the art at the time of the invention. The step at which Atalla teaches this does represent data *"in a communications phase."* Atalla teaches token creation at fig. 1 items 13, 15, 17, 19, 21 where creation of a message authentication code encrypted with a session key is illustrated, and additionally at col. 3 line 60 through col. 4 line 10. Atalla teaches comparison of a MAC and a calculated MAC for authentication purposes in, for example, the abstract.

The applicant argues in traverse of the taking of Official Notice in the rejection of claims under 35 USC 103(a), and asks for a showing of art in support of the taking of Official Notice.

The Examiner took Official Notice in the claimed feature of generation of a pseudo-random number by a block-cipher acting in an output feedback mode. First, the applicant's attention is drawn to claim 12 where the language is found: "...the pseudorandom sequence being generated by operating the block cipher in a known output feedback mode." The Applicant's own claim language anticipates use of a known, i.e., taught by prior art, method of generating a pseudorandom number by this method. Additionally, as a showing of art, the Applicant's attention is drawn to Menezes, Van Oorschot, and Vanstone: "Handbook of Applied Cryptography" (pub. 1996) page 173 Sec. 5.3 Pseudorandom Bit Generation, where generation of pseudorandom values

via a block cipher DES is discussed, Sec. 5.3.1 where the ANSI X9.17 algorithm is discussed, page 250 sec. 7.4 DES, where the DES encryption protocol is described as having been developed in the mid 1970's, page 188, discussion of Sec. 5.3 where the Meyer and Matyas algorithm is discussed, and page 738 where the publication date of Meyer and Matyas is given as 1982. Therefore it can be concluded that generation of pseudorandom sequences via block ciphers operating in feedback mode have been well known in the art for at least the past 30 years.

Motive to make this combination is discussed by Atalla in at least col. 4 lines 5-6 where he contemplates using any "conventional means" for generation of a random number. The technique of generation of a random number by the technique of a block-cipher acting in an output-feedback mode is very well characterized, and is very widely used. It therefore constitutes a *"conventional means"* for the generation of a random number.

Official Notice was taken of the commonality of the use of the "exclusive or" bitwise operation (XOR) in the production of message authentication codes (MAC). As a showing of art, the applicant's attention is now drawn to Zeidler 4,423,287, where such a process is detailed. The motive to make such a combination with Atalla is the rapidity with which such a process can produce a MAC.

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

5. Claims 11-13, 15, 16, 18, 19, 22, 23, 25, 27, and 29 are rejected under 35 U.S.C. 102(b) as being clearly anticipated by Atalla et al., US Patent 5,319,710 Jun. 7, 1994.

As per claim 11, 12, and 15, Atalla teaches a method for transmitting signals between a transmitter and a receiver, the method comprising: Calculating data as a function of a secret key using at least one cryptographic algorithm in a calculation phase, (abstract), Calculating authentication tokens for the signals as a function of the data in a communication phase so as to authenticate both the signals and the transmission sequence of the signals, (abstract, fig. 1, col. 3 line 60 through col. 4 line 10). Atalla teaches generation of a random number (fig. 2A item 52). Atalla teaches a step wherein signals received by a receiver from a transmitter are accepted as authentic if the transmitted authentication token is found to match an authentication token calculated by the receiver (Abstract).

As per claim 13, Atalla teaches certain strings of the pseudo-random sequence are used for coding the signals and positions in the transmission sequence (abstract, fig. 3A, 3B, col. 3 lines 60-68 and col. 4 lines 1-29), and wherein the authentication token of one of the signals transmitted at an i-th position is calculated as a function of

the coding of the signal and coding of the respective position in the transmission sequence (col. 3 line 60 through col. 4 line 29).

As per claims 16 and 25, Atalla teaches certain strings of the pseudo-random sequence are used for coding the signals and positions in the transmission sequence and wherein the authentication token of a one of the signals transmitted at an ith position is calculated as a function of the coding of all previously transmitted signals and the coding of the respective portion in the transmission sequence, (col. 2 line 49 through col. 3 line 25, col. 3 line 60 through col. 4 line 29).

As per claims 18, 19, and 27, Atalla teaches a cryptographic algorithm that includes a block cipher including DES (col. 4 lines 1-29).

As per claims 22, 23, and 29, Atalla teaches calculation of another token for authentication of the transmitter, the other token being subsequently transmitted so as to initialize the receiver for authentication of the transmitter and confirming the transmission sequences by non-intersecting m-bit strings (col. 5 lines 5-38).

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the

invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. Claims 14, 17, 20, and 21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Atalla as applied to claim 11 above, and Official Notice taken as detailed below. Claims 24, 26, 28, and 30 are rejected under 35 USC 103(a) as being unpatentable over Atalla and Official Notice.

8. As per claims 14, 17 and 26, Atalla does not specifically teach the authentication token of the signal transmitted at the ith position is a bit-by-bit XORing of the of the coding of the one signal and the coding of the respective position in the transmission sequence. Atalla does teach such a combination producing the authentication token (col. 3 line 60 through col. 4 line 27) but not use of an XORing process. However the use of XOR functions in producing MAC codes is old and well known in the art or cryptographic authentication routines, therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to have incorporated this feature into the system of Atalla. It would have been desirable due to the simplicity of implementation of the function and it's low computational overhead.

9. As per claims 20, 21 and 28, Atalla does not specifically teach production of a pseudo-random sequence via a block cipher operating in a known output feedback mode. However Official Notice may be taken that generation of pseudorandom sequences in this manner are old and well known in the art. Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate

this feature into the system of Atalla. It would have been desirable to do so as the block cipher is well quantified and the output true randomness can accurately be determined.

10. As per claims 24 and 30, Atalla teaches a method for transmitting signals between a transmitter and a receiver, the method comprising: Calculating data as a function of a secret key using at least one cryptographic algorithm in a calculation phase, (abstract), Calculating authentication tokens for the signals as a function of the data in a communication phase so as to authenticate both the signals and the transmission sequence of the signals, (abstract, fig. 1, col. 3 line 60 through col. 4 line 10). Atalla teaches generation of a random number (fig. 2A item 52) certain strings of the pseudo-random sequence are used for coding the signals and positions in the transmission sequence (abstract, fig. 3A, 3B, col. 3 lines 60-68 and col. 4 lines 1-29) and wherein the authentication token of one of the signals transmitted at an i-th position is calculated as a function of the coding of the signal and coding of the respective position in the transmission sequence (col. 3 line 60 through col. 4 line 29). Atalla teaches a step wherein signals received by a receiver from a transmitter are accepted as authentic if the transmitted authentication token is found to match an authentication token calculated by the receiver (Abstract).

Atalla does not specifically teach the authentication token of the signal transmitted at the ith position is a bit-by-bit XORing of the coding of the one signal and the coding of the respective position in the transmission sequence. Atalla does teach such a combination producing the authentication token (col. 3 line 60 through col. 4 line

27) but not use of an XORing process. However the use of XOR functions in producing MAC codes is old and well known in the art or cryptographic authentication routines, therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to have incorporated this feature into the system of Atalla. It would have been desirable due to the simplicity of implementation of the function and it's low computational overhead. Atalla teaches calculation of another token for authentication of the transmitter, the other token being subsequently transmitted so as to initialize the receiver for authentication of the transmitter and confirming the transmission sequences by non-intersecting m-bit strings (col. 5 lines 5-38).

Conclusion

11. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Paul E. Callahan whose telephone number is (703) 305-1336. The examiner can normally be reached on M-F from 9 to 5.

If attempts to reach the examiner by telephone are unsuccessful, the Examiner's supervisor, Andrew Caldwell, can be reached on (703) 306-3036. The fax phone number for the organization where this application or proceeding is assigned is: (703) 872-9306. Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-3900.

9/26/04

Paul Callahan